International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 2, Issue 12, December 2015

Cooperative Message Authentication Used In L-P2dsa

Riya Baby
PG Scholar (Electronics and Communication Department)
Mar Baselios Institue Of Technology

Abstract: VANET is a special kind of MANET. It will provide communication between vehicles and fixed units and also among the vehicles . VANETs are mainly used for Traffic optimization and improving safety. Due to open nature of wireless medium, a lot of attacks are possible in vanet. In this paper we propose a method to reduce the overload of DMV and vehicle. To improve the computation overhead in DMV, we use 2 hash values and location of vehicle. In the case of vehicle we use co-operative message authentication method.

I. INTRODUCTION

Million people are killed each year on the road accidents. Road traffic safety is the challenging issue in traffic management. One method is to overcome this situation by exchanging the information of traffic environment among the vehicles. VANET is self organized network that can be formed by connecting vehicle, to improve driving safety and traffic management with internet access by drivers.

VANET represents a challenging class of MANET that enables vehicle to vehicle communication and vehicle to roadside unit communication. VANETs are playing an important role in accident avoidance, traffic control, and management of parking vehicle in public area. To develop a cooperation based system, give more importance to security and privacy.

To secure the VANET, first we have to discover who are the attacker, their capacity, and nature to damage the system. On the basis of capacity these attackers may be three types. Insiders are the authenticated members of n/w and Outsiders are the intruders and hence limited capacity to attack. These types of attackers are an authentic user of the network and have detail knowledge of network. One of the very important attack is Sybil attack.In this paper we discuss about location based method to avoid Sybil attack and also reduce the work load of the DMV.

Malicious attackers have not any personal benefit to attack; they just harm the functionality of the network. Sometimes they make the vehicle receiver busy by sending unwanted messages. A single vehicle is verify all the messages they take more time and important messages some time can't get. So to avoid this problem we use cooperative message authentication method. It will help to reduce the workload of vehicle.

II. LOCATION-BASED PRIVACY PRESERVING DETECTION

Sybil attacks means number of vehicle have same identity. So the DMV have higher number of computation is for finding attacker. To avoid the overload working of DMV we introduce RSU. In this case we use different hash values. But for reducing the storage capacity we did not store the complete hash value. In the RSU we store a small portion of hash value. It is created by using public key given by DMV. Mainly this value is hacked so we change it in every week.DMV store a small portion of another hash value. It is created by using privet key.

If 2 different pseudonyms indicate same position in RSU hash value table. It indicates some suspicious thing is occur. Then it checks the position of the vehicle. If they are in the different places we consider it as a misunderstanding.

If they are in the same location we inform in to the DMV. If hash value present in the DMV hash value table. We consider it as a real one otherwise it is an attacker.

III. COOPERATIVE MESSAGE AUTHENTICATION

Compared with the conventional non-cooperative message authentication protocol, our CMAP method achieves significantly lower computation overhead. Based on a practical 2-dimensional road map, we compare the direction of message send vehicle with neighboring vehicle and discarded the message which is not in the same direction.

Then using verifier protocols, vehicles will decide whether they are verifiers of this message or not. In the verifier protocol we check the distance from the sender and shortest distance vehicle will select as verifier. Sometimes it may be more than one. If a vehicle is the verifier of the message, it will start to verify the message by itself. That is it will check the identity is presented in the attacker list. If it identified the identity, broadcast a warning msg. Otherwise, verifiers will keep silent. Non-verifiers will wait for cooperative warning messages (CWM) from verifiers. When a non-verifier receives a CWM from other vehicles, it will double check the corresponding message. Non-verifiers will consume the message if it does not receive any CWM from

others within 100 ms.

CONCLUTION

In this paper explain how to reduce the work load in DMV and vehicle. That is to avoid Sybil attack and DOS attacks. In this two approach we consider the position of vehicle. Vehicles is moving in the different direction will discard the unwanted message. By this method we can reduce the workload of vehicle.

ACKNOWLEDGMENT:-

The author would like to thank teachers and friend in Mar Baselios Institue of Technology.

REFERENCES

1.Qi Yang, Zhixue He, Zhu Yang, Shaohua Yu, Xingwen Yi, and William Shieh. Coherent optical DFT-Spread OFDM transmission using orthogonal band multiplexing 30 January 2012 / Vol. 20, No. 3 / OPTICS EXPRESS 2380

2.Xi Chen,1,* An Li, Guanjun Gao,and William Shieh.Experimental demonstration of improved fiber nonlinearity tolerance for unique-word DFT-spread OFDM systems. 19 December 2011 / Vol. 19, No. 27 / OPTICS EXPRESS 26198

3.Chun-Ting Lin*,Yu-Min Lin, Jason(Jyehong)Chen, Sheng-Peng Dai Po Tsung Shih,Peng-Chun Peng, and Sien Chi. Optical direct-detection OFDM signal generation for radio-over-fiber link using frequency doubling scheme with carrier suppression. 28 April 2008 / Vol. 16, No. 9 / OPTICS EXPRESS.

4.Ma Tao, Li Wanlin, Jiao Qun, Chen Jun. Research on High-precise time transmission system over optical fiber. 978-1-4244-8694-6/11/$26.00 ©2011 IEEE

5.Ezra Ip*, Alan Pak Tao Lau, Daniel J. F. Barros, Joseph M. Kahn. Coherent detection in optical fiber systems. 21 January 2008 / Vol. 16, No. 2 / OPTICS EXPRESS 753